

REMARKS

Claims 16-36 are pending in the current application. Claims 1-15 are canceled. Claims 16 and 28 are independent claims. Claims 25 and 26 are amended.

Claim Objections

Claims 25 and 26 are objected to because of the following informalities: Each claim is recited as being dependent on “any of the claims,” but only one claim is listed. Claims 25 and 26 have been amended to address the objections noted by the Examiner.

Claim Rejections – 35 U.S.C. § 102

Claims 16, 18, 22, 25, 28, 29 and 32-35 stand rejected under 35 U.S.C. § 102(b) as being anticipated by Caronni et al. (US 6,049,878, hereinafter “Caronni”).

Applicants respectfully submit Caronni fails to teach each of the elements of claim 1 as is required to support a rejection under §102. Claim 1 recites: “encryption and transmission of at least two cryptograms each comprising the temporary encryption key, the first cryptogram being encrypted under the unique authorisation key of a non-revoked security module and the second cryptogram being encrypted by a group authorisation key pertaining to a group of security modules to which the revoked security module does not belong”. With respect to these limitations, the Examiner directs Applicants attention to col. 9, lines 1-24 of Caronni which describe a key distribution process in which a message 600 is sent to update keys for participants in the key hierarchy displayed in FIG. 4 of Caronni. As FIG. 6 of Caronni illustrates, new keys K45', K47' and TEK' are all encrypted and included in message 600. However, none of these keys is encrypted by **both a unique key and a group key** as claim 1 requires. Referring to FIG. 6 of Caronni, Key K45' is encrypted by unique key X4. Key K45' is not encrypted by any other

keys. Accordingly, key K45' is not encrypted by both a unique key and a group key. Key K47' is encrypted by keys K45' and K67. Keys K45' and K67 are both shared keys. Neither of keys K45' and K67 are unique keys. Accordingly, key K47' is not encrypted by both a unique key and a group key. Key TEK' is encrypted by keys K03 and K47'. Keys K03 and K47' are both shared keys. Neither of keys K03 and K47' are unique keys. Accordingly, key TEK' is not encrypted by both a unique key and a group key (Caronni: col. 9 ln. 1-25). Consequently, Caronni cannot teach encrypting a temporary key with both a unique key and a group key as claim 1 requires.

Further, Applicants would also like to direct the Examiner's attention to a fundamental difference between Caronni and the subject matter of claim 1. Both the subject matter of claim 1 and Caronni relate to securely transmitting encrypted data to a plurality of receiving entities. Both relate to grouping receiving entities into hierarchical tree structures and using both group encryption keys and unique encryption keys for the receiving entities. However, a fundamental difference is that the subject matter of claim 1 allows for a receiving unit to be precluded from being able to decrypt data without a need to re-attribute new encryption keys. Column 8, line 27-30 of Caronni states "In response, the group key manager component 108 identifies all the keys known by the participants(s) 101 that are to be thrown out. All of those keys need to be replaced by new versions". Caronni requires the sending of $2 \cdot \log_2(n-1)$ encryptions once a participant leaves to send new keys for an arbitrary number N participants (Caronni: col. 9, ln. 10-27). On the contrary, the subject matter of claim 1 allows for a receiving entity's rights to be revoked by simply no longer using keys known to the revoked receiving entity. No new keys need to be issued.

Accordingly, at least for the reasons stated above, Caronni fails to teach each of the elements of claim 1 as is required to support a rejection under §102.

Additionally, claim 28 contains limitations similar to those of claim 1. Accordingly, at least by virtue of its similarity to claim 1, Caronni fails to teach each of the elements of claim 28 as is required to support a rejection under §102.

Further, claims 16, 18, 22, 25, and 33 depend from claim 16; and claims 29, 32, 34 and 35 depend from claim 28. Accordingly, at least by virtue of their dependence from claims 16 and 28, Caronni fails to teach each of the elements of any of claims 16, 18, 22, 25, 29, 32, 33, 34 and 35 as is required to support a rejection under §102.

Therefore Applicants respectfully request the rejections of claims 16, 18, 22, 25, 28, 29 and 32-35 under 35 U.S.C. §102 be withdrawn.

Claim Rejections – 35 U.S.C. § 103

Claims 17 and 19 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Caronni.

For at least the reasons stated above, Caronni fails to teach each of the limitations of claim 1. Accordingly, at least by virtue of their dependence from claim 1, Caronni fails to teach each of the limitations in either of claims 17 and 19 as is required to support a *prima facie* case of obviousness. Consequently, the Examiner cannot establish a *prima facie* case of obviousness with respect to either of claims 17 and 19 as is required to support a rejection under §103.

Therefore Applicants respectfully request the rejections of claims 17 and 19 under 35 U.S.C. §103 be withdrawn.

Claims 20, 21, 23, 24, 26, 27, 30 and 31 stand rejected under 35 U.S.C. § 103(a) as being unpatentable over Caronni as applied to claim 16 above, and further in view of Campinos et al. (US 6,035,038, hereinafter “Campinos”).

The deficiencies of Caronni are discussed above and are relevant here because claims 20, 21, 23, 24, 26 and 27 depend from claim 16; and claims 30 and 31 depend from claim 28. Campinos fails to remedy those deficiencies at least because Campinos likewise fails to teach “encryption and transmission of at least two cryptograms each comprising the temporary encryption key, the first cryptogram being encrypted under the unique authorisation key of a non-revoked security module and the second cryptogram being encrypted by a group authorisation key pertaining to a group of security modules to which the revoked security module does not belong” as is required by claims 16 and 28. Accordingly, neither Caronni nor Campinos, alone or in combination, teaches each of the limitations in either of claims 16 and 28 as is required to support a *prima facie* case of obviousness. Consequently, at least by virtue of their dependence from claims 16 and 28, the Examiner cannot establish a *prima facie* case of obviousness with respect to any of claims 20, 21, 23, 24, 26, 27, 30 and 31 as is required to support a rejection under §103.

Therefore Applicants respectfully request the rejections of claims 20, 21, 23, 24, 26, 27, 30 and 31 under 35 U.S.C. §103 be withdrawn.

CONCLUSION

Accordingly, in view of the above amendments and remarks, reconsideration of the objections and rejections and allowance of each of claims 16-35 in connection with the present application is earnestly solicited.

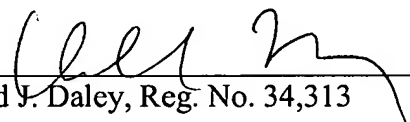
Should there be any outstanding matters that need to be resolved in the present application, the Examiner is respectfully requested to contact Donald J. Daley at the telephone number of the undersigned below.

If necessary, the Commissioner is hereby authorized in this, concurrent, and future replies, to charge payment or credit any overpayment to Deposit Account No. 08-0750 for any additional fees required under 37 C.F.R. § 1.16 or under 37 C.F.R. § 1.17; particularly, extension of time fees.

Respectfully submitted,

HARNESS, DICKY, & PIERCE, P.L.C.

By


Donald J. Daley, Reg. No. 34,313

P.O. Box 8910
Reston, Virginia 20195
(703) 668-8000

JHA
DJD/JHA: tlt